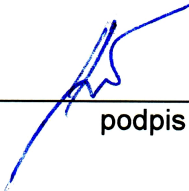
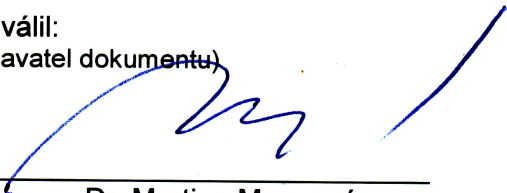
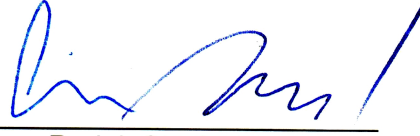


CVP – P – 06		Výtisk č.:
		Počet stran: 8
Účinnost od:	Doba platnosti:	Rozsah platnosti:
1. 9. 2019	do odvolání	Vysoká škola regionálního rozvoje a Bankovní institut – AMBIS, a.s.
<p>Název dokumentu:</p> <p style="text-align: center;">PROVOZNÍ ŘÁD INFORMAČNÍHO SYSTÉMU</p> <p>Zpracoval: (garant dokumentu)</p> <p style="text-align: center;">Ing. Milan Hála</p> <div style="text-align: center;">  _____ podpis </div> <p>Schválil: (vydavatel dokumentu)</p> <div style="display: flex; justify-content: space-around;"> <div style="text-align: center;">  _____ Dr. Martina Mannová členka představenstva </div> <div style="text-align: center;"> Dne: 1. 9. 2019  _____ Radek Stavinoha člen představenstva </div> </div>		
Počet příloh:	0	Názvy příloh:
Číslo vydání:	2.	
Druhé	Nahrazuje: — CVP-P-06 Provozní řád informačního systému ze dne 1. 4. 2019	



Čl. I

Úvodní ustanovení

- (1) Tato směrnice určuje závazná pravidla provozu informačního systému Vysoké školy regionálního rozvoje a Bankovního institutu – AMBIS, a.s. (dále „VŠ AMBIS“), pravidla pro užívání software a elektronickou komunikaci.
- (2) Smyslem směrnice je zajistit bezporuchový a bezpečný provoz výpočetní techniky, zajistit všem oprávněným uživatelům přístup k IT službám a k potřebnému software, zamezit poškození nebo zneužití dat, zajistit efektivní využití výpočetní techniky k plnění pracovních úkolů.
- (3) Součástí této směrnice jsou bezpečnostní standardy, ve kterých jsou blíže specifikovány požadavky a pravidla vycházející z jednotlivých částí této směrnice.

Čl. II

Použité pojmy

- (1) Prostředek výpočetní techniky (výpočetní prostředek) je jakékoliv zařízení připojitelné do počítačové sítě – např. osobní počítač, notebook, tiskárna, scanner apod.
- (2) Informační systém (IS) je vzájemně propojený systém prostředků výpočetní techniky a software, který slouží ke zpracovávání a poskytování informací.
- (3) Správce informačního systému (dále jen správce) je osoba nebo organizace odpovědná za správu a provoz informačního systému.
- (4) Oprávněný uživatel informačního systému (dále jen uživatel) je každý zaměstnanec a student VŠ AMBIS, který používá výpočetní techniku a programové vybavení k výkonu své funkce či studiu, jeho konkrétní oprávnění jsou dána nastavením přístupových práv.

Čl. III

Informační systém AMBIS

- (1) Prostředky výpočetní techniky na VŠ AMBIS jsou propojeny do lokální datové počítačové sítě, která je centrálně spravována. Tato počítačová síť umožňuje vzájemnou komunikaci jednotlivých prostředků, sdílení zdrojů a informací.
- (2) Provoz informačního systému VŠ AMBIS (dále jen „IS“) zajišťuje externí společnost Adineo, s. r. o., se sídlem Roháčova 1095/77, 130 00 Praha 3, prostřednictvím pověřené osoby (dále jen „správce“).
- (3) Organizačně je správa IS přičleněna provoznímu a projektovému úseku, přes který uživatel se správcem komunikuje. Veškeré požadavky a sdělení správci uživatel směřuje provoznímu a projektovému úseku (provoznímu manažerovi). Pokud je v této směrnici uvedeno „sdělí správci“ znamená „sdělí správci prostřednictvím provozního a projektového úseku zpravidla e-mailem na adresu provoz@ambis.cz“.
- (4) Informační systém je provozován nepřetržitě v režimu 24 hodin / 7 dní v týdnu.
- (5) Informační systém je provozován na následujících pobočkách VŠ AMBIS:
 - A. sídlo společnosti (pobočka Libeň) – Lindnerova 575/1, 180 00 Praha 8 – Libeň
 - B. pobočka Brno – Mezírka 775/1, 602 00 Brno – střed
- (6) V pobočce A jsou umístěny hlavní servery v uzamčené místnosti serverů, v pobočce B je umístěn detašovaný servery, rovněž v uzamčené místnosti. K serverům mají přístup jen pověřené osoby, o přístupu rozhoduje provozní manažer. Propojení serverů je realizováno pomocí šifrovaného spojení prostřednictvím veřejné sítě internet.
- (7) V budově A a v pronajatých prostorách budovy B je proveden rozvod strukturované kabeláže do každé místnosti. Jednotlivé přípojné místa do LAN jsou připojena k serverům přes datové rozvaděče a je možné nastavení přístupových práv.



- (8) Všechny budovy jsou pokryty signálem WiFi ve dvou oddělených sítích (studentské a provozní). Přístupy do studentské sítě jsou zveřejněny v informačním systému pro všechny studenty a zaměstnance školy. Přístup do provozní sítě je regulován, přístup povoluje na základě potřeby či žádosti provozní manažer. Pro každou z obou sítí jsou z důvodu ochrany sítě nastavena rozdílná práva.
- (9) Pro studenty je možný přístup k internetu a do IS buď v počítačových učebnách na jednotlivých pracovištích školy nebo prostřednictvím WiFi připojení. Akademickým pracovníkům jsou k dispozici vyhrazené počítače v pracovnách, nebo mohou využít WiFi síť. Provozní zaměstnanci mají podle charakteru své práce přidělen buď „pevný“ počítač nebo notebook. Po přihlášení do IS jsou jim zpřístupněny sdílené složky na serverových discích dle jejich funkčních oprávnění (přístupových práv).
- (10) Pracovníkům školy jsou k dispozici tiskárny umístěné na jednotlivých pracovištích nebo na chodbě školy. Je zakázáno užívat tiskárny v prostorech přístupných studentům pro tisk dokumentů obsahujících osobní údaje.
- (11) Správce zodpovídá za vývoj a provoz IS v souladu s platnými právními předpisy a dalšími závaznými dokumenty. Společně s provozním manažerem stanovuje podmínky provozu IS, vytváří obecná pravidla pro zpracovávání, využívání a zveřejňování dat a informací a jejich zabezpečení.
- (12) Na VŠ AMBIS jsou v režimu outsourcingu využívány další informační systémy, jejichž popis je uveden v této směrnici.

Čl. IV

Externí dílčí IS využívané na VŠ AMBIS

- (1) Na VŠ AMBIS jsou využívány další informační systémy.
- (2) Na serverech VŠ AMBIS
 - finanční úsek využívá ekonomický systém HELIOS Inuvio,
 - úsek certifikace využívá inf. systém pro správu certifikovaných osob.
- (3) V režimu outsourcingu:
 - studijní informační systém provozovaný Masarykovou univerzitou dostupný na <https://is.ambis> (studijní oddělení).
 - systém telefonní ústředny OptimSys (studijní a zákaznické oddělení),
 - CRM systém RAYNET (zákaznické oddělení).
- (4) Zaměstnanci VŠ AMBIS dále prostřednictvím IS přistupují k informačním systémům třetích stran. Pro přístup k těmto systémům musí dodržovat pravidla správců těchto systémů.

Čl. V

Práva a povinnosti uživatele

- (1) Práva uživatele IS:
 - přistupovat k software v IS v rozsahu svých pracovních činností nebo studijních povinností,
 - podávat návrhy, podněty a stížnosti související s provozem IS a s porušováním této směrnice správci IS.
- (2) Povinnosti uživatele:
 - řídit se pokyny správce,
 - seznámit se s provozem IS v potřebném rozsahu,
 - chránit a udržovat přidělené prostředky výpočetní techniky,
 - užívat prostředky IS pouze k plnění svých pracovních nebo studijních povinností v souladu s účelem, ke kterému byly tyto prostředky určeny,
 - neprovádět žádné změny v konfiguraci přiděleného vybavení,



- neinstalovat žádný další software,
- oznámit správci nestandardní chování IS, potřebu provedení opravy či aktualizace software či hardware,
- zabezpečit propůjčené prostředky IS fyzicky proti poškození či odcizení,
- pracovat obezřetně s přenosnými médii a elektronickou poštou s ohledem na ochranu údajů či riziko nákazy škodlivým software,
- ukládat data, se kterými pracuje, do stanovených úložišť (na sdílené disky),
- zpřístupnit přidělené prostředky IS správci v souvislosti s technickou správou sítě, kontrolou dodržování povinností uživatele či upgrade kdykoliv je k tomu vyzván,
- používat pouze software, který je na jeho počítači správcem nainstalován, v případě potřeby jiného software se obrátit na správce,
- neměnit žádné informace s cílem ovlivnit kontrolu oprávněnosti použití software,
- nešířit software, který je součástí IS,
- dbát ochrany dat ve smyslu nařízení Evropského parlamentu a Rady 2016/679 a zákona o ochraně osobních údajů,
- neposkytovat žádné jemu propůjčené prostředky výpočetní techniky jiným osobám bez souhlasu správce,
- chránit přístupové údaje do IS a nesdělovat je žádné jiné osobě (včetně správce); v případě porušení tohoto pravidla odpovídá za změny, které byly provedeny pod jeho uživatelským jménem.

Čl. VI

Práva a povinnosti správce

(1) Práva správce:

- provádět změny programového vybavení na klientských počítačích,
- vydávat pokyny uživatelům související s provozem IS, zejména v případě výskytu závady a vyžadovat jejich plnění,
- odepřít přístup k službám IS těm uživatelům, kteří porušují tuto směrnici nebo nedodržují jeho pokyny, prostřednictvím administrace uživatelských účtů – o odepření přístupu neprodleně informuje provozního manažera,
- provádět vývoj a úpravy IS na základě pokynů provozního manažera.

(2) Povinnosti správce

- provádět správu systému tak, aby byla zajištěna jeho co nejvyšší dostupnost,
- zabezpečit všem uživatelům přístup k software v rozsahu jejich pracovních nebo studijních povinností,
- zajistit ochranu všech uložených dat na serverech před zneužitím, poškozením, ztrátou a zničením,
- provádět činnosti související s konfigurací a administrací IS podle pokynů provozního manažera,
- provádět činnosti související s technickou správou klientských počítačů a dalších prostředků výpočetní techniky,
- provádět administraci uživatelských účtů a zajistit přístup uživatelů IS do systému v rozsahu, který jim byl povolen,
- provádět zálohování a archivaci dat podle stanoveného plánu.
- spravovat systémové auditní záznamy v IS včetně jejich zabezpečení proti zneužití, přístup k těmto záznamům umožní pouze osobám, které určí vedení společnosti,
- dohlížet na dodržování této směrnice všemi uživateli,
- zabezpečovat školení uživatelů,
- informovat uživatele o změnách v IS, pokud to ovlivní plnění jeho pracovních nebo studijních povinností.



ČI. VII

Pravidla provozu IS

- (1) Přístup do IS je umožněn pouze uživatelům, kteří se přihlásí pomocí svých přihlašovacích údajů na libovolném počítači připojeném v IS. Přihlášením uživatel získává přístup k jemu určeným prostředkům. Přihlášení je možné i vzdáleně s využitím VPN.
- (2) Každému uživateli je správcem vytvořen uživatelský účet, ke kterému jsou přiřazena oprávnění odpovídající pracovnímu zařazení (práva k aplikacím a práva ke sdíleným složkám). Požadovaná oprávnění pro zaměstnance sdělí správci vedoucí personálního úseku. Protože práva jsou definována příslušností uživatele ke skupinám Active Directory, které definují organizační příslušnost uživatele nebo jeho roli.
- (3) Studenti k přihlášení v počítačových učebnách používají jednotné přihlašovací údaje. Samostatné účty nejsou vytvářeny.
- (4) Správce na základě pokynu personálního úseku přidělí uživateli uživatelské jméno a počáteční přístupové heslo. Počáteční heslo musí být uživatelem při prvním přihlášení změněno.
- (5) Uživatel nesmí své přihlašovací údaje sdělovat jiným osobám. V případě kompromitace nebo zapomenutí hesla oznámí uživatel tuto skutečnost správci, který přidělí uživateli nové počáteční heslo. V případě, že uživatel tyto údaje sdělí neoprávněným osobám, je zodpovědný za škody, které budou způsobeny zneužitím jeho přístupových údajů.
- (6) Uživatelům je zakázáno do IS připojovat vlastní zařízení (např. mobilní) bez souhlasu správce. To neplatí pro připojení k WiFi pouze za účelem připojení k internetu (osoba, připojená pouze k WiFi není chápána jako uživatel podle této směrnice).
- (7) Uživatel, kterému je odepřen přístup do IS, sdělí tuto informaci správci, který ověří příčinu a sdělí uživateli další postup.
- (8) Pokud je uživatel přihlášen k IS, nesmí ponechat počítač bez dohledu. Při opuštění pracoviště musí přístup k IS uzamknout či počítač vypnout.
- (9) Pokud uživatel zjistí nestandardní chování IS nebo jeho části (nedostupnost, zpomalení, obava z činnosti škodlivého kódu), informuje neprodleně správce. Správce oznámí, kdy začne s řešením problému a prognózu času odstranění, přičemž si bude počínat tak, aby byly minimalizovány dopady na práci uživatele.
- (10) Instalaci software provádí pouze správce nebo jím pověřená osoba, stejně tak aktualizace nebo další změny.
- (11) Při opakovaném porušování povinností a výše uvedených pravidel budou proti uživateli uplatňována odpovídající opatření a správce může se souhlasem provozního manažera rozhodnout o dočasném odebrání přístupových práv uživateli. Správce musí o takovém kroku vždy informovat personální úsek.

ČI. VIII

Bezpečnost dat, zálohování

- (1) Za bezpečnost, ochranu před zneužitím, zcizením či ztrátou dat uložených ve stanovených úložištích (na datových a souborových serverech) odpovídá správce.
- (2) Za bezpečnost dat uložených na lokálních discích osobních počítačů odpovídají jednotliví uživatelé. Tím se nezbuývají povinnosti ukládat data do stanovených úložišť (sdílené disky).
- (3) Správce může nastavit limit pro ukládání dat pro jednotlivé úseky společnosti / uživatele.
- (4) Při vyřazování počítačů a jejich následném odprodeji či likvidaci správce zajistí, že na pevném disku či jiném paměťovém médiu nebudou žádná data. O vyřazení počítače a způsobu likvidaci dat vytvoří správce protokol, který bude provozním a projektovým



úsekem řádně uložen. Obdobně postupuje správce i případě, kdy je výpočetní prostředek přidělen jinému uživateli.

Čl. IX

Pravidla pro užívání počítačových programů

- (1) Získání a užívání softwaru se řídí především ustanoveními zákona č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) ve znění pozdějších předpisů a licenčním ujednáním (smlouvou), která je k softwaru připojena.
- (2) Software musí být pořizován v souladu s platnými zákony a dalšími předpisy. K zajištění oprávněnosti používat nakoupený software je nutné:
 - software, pokud nebyl vytvořen v rámci VŠ AMBIS, pořizovat pouze u výrobců či jimi autorizovaných distributorů a požadovat od dodavatelů potřebná ujištění v rámci smluv na dodávky počítačových programů,
 - v případě, že je software na nakoupeném hardware předinstalován, požadovat od dodavatelů písemná potvrzení o legalitě předinstalovaného software,
 - k software požadovat originální instalační média a uživatelskou dokumentaci s výjimkou počítačových programů distribuovaných pouze elektronicky,
 - řádně evidovat originální smluvní, licenční a jiná ujednání v rozsahu umožňujícím prokázání oprávněnosti užívání software,
 - řádně registrovat zakoupený software, pokud je registrace výrobcem požadována,
 - software užívat pouze v souladu s licenčním ujednáním,
 - v případě vyřazení software nebo zániku platnosti licencí znemožnit další používání tohoto software. V případě že je počítačový program svázan s daty, které je třeba uchovat zajistit, aby software nebyl neoprávněně používán.
- (3) Základním dokladem o oprávněném použití software je zaplacená faktura. Oprávněnost používání počítačových programů lze dále prokázat:
 - smlouvami o dodávce,
 - nabývacími doklady,
 - licenčními smlouvami upravujícími užívání,
 - doklady o registraci software,
 - elektronickými kopiemi odeslaných a přijatých zpráv v případě pořízení programu dálkovým přístupem.
- (4) Dokumenty prokazující oprávněnost použití software musí být řádně evidovány.

Čl. X

Pravidla elektronické komunikace

- (1) Elektronická komunikace slouží pro zrychlení a zkvalitnění toku informací uvnitř i vně společnosti. Zprávy a dokumenty, poskytované či zveřejňované touto cestou, musí splňovat požadavky na chování požadovaného u zaměstnance či studenta VŠ AMBIS.
- (2) Pro každého zaměstnance VŠ AMBIS, který má zřízen přístup do IS, je zřízena elektronická poštovní schránka (e-mail). Poštovní systém je provozován v systému Microsoft Office 365. Zaměstnanci jsou povinni používat tento způsob komunikace výhradně ke služebním účelům.
- (3) Formát elektronické adresy zaměstnance: jmeno.prijmeni@ambis.cz. Pokud byla odpovídající kombinace jmeno.prijmeni již použita, doplní se vhodným způsobem (např. jmeno.prijmeni2).
- (4) Studentům je vytvořena e-mailová schránka po zavedení do studijního informačního systému s adresou ve tvaru uco@mail.ambis.cz, kde uco je jedinečný identifikátor každé osoby využívající studijní informační systém. Student je používat pro komunikaci s VŠ AMBIS tento e-mail.



- (5) Pro zabezpečení elektronické pošty od vnějších subjektů jsou na Ambis zřízeny následující e-mailové schránky:
 - info@ambis.cz (spravuje zákaznické oddělení),
 - studijni@ambis.cz (spravuje studijní oddělení),
 - econ@ambis.cz, fakturace@ambis.cz, finance@ambis.cz (spravuje finanční úsek),
 - pohledavky@ambis.cz (spravuje finanční úsek spolu se studijním oddělením),
 - provoz@ambis.cz (spravuje provozní a projektový úsek,
 - další e-mailové adresy podle potřeb provozu školy zabezpečuje a přístupová práva nastavuje provozní a projektové oddělení.
- (6) VŠ AMBIS má zřízenou datovou schránku typu OVM – Právnícká osoba s ID ftxc2jx. Přístup do datové schránky mají členové představenstva a jimi pověřené osoby. Předávání zpráv doručených do této schránky a jejich další doručení podle konkrétního obsahu se provádí dle ustanovení Spisového řádu VŠ AMBIS.
- (7) Přístup k Internetu – konektivita poboček VŠ AMBIS k internetu je zajištěna externími dodavateli:
 - budova A – Praha – Libeň: ÚVT Internet s.r.o., Hrnčířská 383, Jesenice-Zdiměřice
 - budova B – Brno: FASTER CZ spol. s r. o., Jarní 1064/44g, 614 00 Brno – Maloměřice a Obřany
- (8) K internetu může každý zaměstnanec přistupovat ze služebního počítače (PC, notebook) po připojení k pevnému rozvodu nebo přes WiFi. K připojení přes WiFi může rovněž použít služební či soukromý telefon či tablet. Všechny uživatelské aktivity jsou zaznamenávány do auditních logů s možností zpětné kontroly jím navštívených stránek.
- (9) Uživatelům je zakázáno stahovat, spouštět nebo instalovat jakýkoliv software bez souhlasu provozního manažera nebo jím pověřené osoby.
- (10) Studenti mohou k internetu přistupovat pouze prostřednictvím WiFi sítě dostupné v pobočkách VŠ AMBIS.
- (11) Správce je oprávněn omezit přístup k síti internet v případech porušování těchto zásad, pravidel bezpečnosti nebo z důvodu neúměrného a neodůvodněného zatěžování přenosové linky uživatelem IS.

Čl. XI

Bezpečnostní standardy

- (1) Součástí této směrnice jsou bezpečnostní standardy, ve kterých jsou blíže specifikovány požadavky a pravidla vycházející z jednotlivých částí této směrnice.

Čl. XII

Seznam souvisejících dokumentů

Tento dokument vychází z následujících dokumentů:

- Organizační řád VŠ AMBIS,
- Spisový řád VŠ AMBIS,
- zákon č. 111/1998 Sb., o vysokých školách a o změně a doplnění dalších zákonů (zákon o vysokých školách).

Čl. XIII

Závěrečné ustanovení

- (1) Tato směrnice je závazná pro všechny zaměstnance, studenty a další osoby, které využívají přístup do IS.
- (2) Součástí této směrnice jsou bezpečnostní standardy, ve kterých jsou upřesněny požadavky či postupy vycházející z této směrnice.



(3) Směrnice je platná ode dne podpisu a její účinnost je uvedena na titulní stránce.

Čl. XIV
Rozdělovník

- (1) Výtisk č. 1 správcovský výtisk
- (2) Výtisk č. 2 výtisk na zápůjčku